Doo" Vodovod i kanalizacija " Herceg Novi
Broj: 04-327/25
Herceg Novi, 04.02.2025.g

UGOVOR O JAVNOJ NABAVCI

Naručioca Doo" Vodovod i kanalizacija " Herceg Novi ulica :Put X hercegovačke brigade br 3, PIB: 02293196, Matični broj: 02293196, Broj računa: 510-169-18, CKB Podgorica, , koga zastupa izvrsni direktor, Boro Lučić, (u daljem tekstu: Naručilac)

i

Ponuđača : ADVANCED CYBER SECURITY doo , Beograd, RSrbija Rudnička 8, Vračar, Beograd, PIB - 111876558 , tel: +381114231957, email: office@acs.co.rs , Žr br: RS35265100000024719822 ADVANCED CYBER SECURITY , koga zastupa Aleksandar Kotevski, izvršni direktor , (u daljem tekstu: Izvršilac usluga).

OSNOV UGOVORA:

Zahtjev za dostavljanje ponuda jednostavne nabavke , postupak ESJN 85668 od 31.12.2024.g za nabavku usluga - Implementacija platforme za rano prepoznavanje IT bezbednosnih incidenata , obavjestenja o ishodu posupka broj : 05-326/25 od 04.02.2025.g najpovoljnija ponuda broj ESJN: 120652 od 16.11.2025. , ponuđača ADVANCED CYBER SECURITY doo ,Beograd, RSrbija , su sastavni dio ovog Ugovora .

Član 1

Izvršilac usluga se obavezuje da NARUČIOCU izvrsiti usluge po Zahtjevu za dostavljanje ponuda jednostavne nabavke , postupak ESJN 85668 od 31.12.2024.g za nabavku usluga - Implementacija platforme za rano prepoznavanje IT bezbednosnih incidenata , obavjestenja o ishodu posupka broj : 05-326/25 od 04.02.2025.g, najpovoljnija ponuda broj ESJN: 120652 od 16.11.2025. , ponuđača ADVANCED CYBER SECURITY doo ,Beograd, RSrbija :
Implementirana platforma za rano prepoznavanje IT bezbednosnih incidenata ISPUNJAVA sledeće funkcionalne zahteve: Prikupljanje i analiza podataka i obaveštavanje o incidentima • Prihvatanje, pohranjivanje i analiza događaja u realnom vremenu poslatih sa postojecih IT sistema (OS radnih stanica, OS servera, rutera, aplikacija, baze podataka, web servera, IDS sistema, firewall-a i dr.). • Brza pretraga, kroz velike količine podataka u cilju digitalne forenzike cyber incidenata • Sistem mora da podrži analizu neograničene količine podataka, limitirane isključivo hardverskim kapacitetima, dok softver ne sme da ima ograničenja u količini podataka za analizu pretraživanja • Pohranjivanje podataka u sledecim oblicima: o originalni tekstualni oblik (originalni, nepromenjen oblik podataka koji ce se automatski arhivirati i koristiti pre svega za pravne potrebe); o goli pretraživi podaci (originalni oblik podataka sa dodatnim meta podacima

vezanim za način prijema , sa mogućnošću brze pretrage); o parsirani podaci (analizirani podaci na osnovu konteksta i/ili sintaksne strukture u cilju brze pretrage i korelacije događaja); o obogaćeni događaji (originalni događaji kojima se dodaju u realnom vremenu kritične informacije nastale na osnovu korelacije); o sintetički događaji: podaci nastali putem korelacije originalnih podataka. • Platforma za rano prepoznavanje IT incidenata predstavlja ključni element u savremenom informacionom društvu, osiguravajući brzu i efikasnu identifikaciju potencijalnih pretnji i problema u okviru IT okruženja. S obzirom na sve veći broj sajber napada i bezbednosnih izazova, potreba za sopstvenim alatom koji će aktivno monitorisati, analizirati i odgovarati na incidente postaje kritična. U tom kontekstu, ključna specifikacija koja se zahteva za ovakvu platformu je integracija i korišćenje standardizovanog formata IDMEF (Intrusion Detection Message Exchange Format), kako je definisano u IETF RFC 4765. IDMEF predstavlja standard koji omogućava uniformnost u obliku poruka koje se koriste za izvestavanje o sigurnosnim incidentima. Specifičnost ovog formata je u njegovoj univerzalnosti - on ne samo što podstiče saradnju i integraciju između različitih sigurnosnih sistema, već takođe omogućava upoređivanje i korelaciju upozorenja iz više heterogenih izvora, poput različitih operativnih sistema, mrežnih uređaja, aplikacija, i drugih sistema. Ovo je posebno značajno u detektovanju složenih napada koji zahtevaju analizu preko više sistema. Navedena platforma, s tim u vidu, mora imati sposobnost da transformiše klasične logove, koji su proizvedeni od strane različitih izvora (OS radnih stanica, OS servera, rutera, aplikacija, baza podataka, web servera, IDS sistema, firewall-a i dr.) u IDMEF upozorenja. Ova konverzija omogućava standardizaciju svih sigurnosnih upozorenja, što doprinosi efikasnijoj obradi i odgovoru na incidente. Dalje, interfejs platforme mora biti dizajniran tako da pruža intuitivan i jasan pristup svim sigurnosnim upozorenjima koja se generišu, s obzirom na to da IT stručnjaci treba da imaju mogucnost da brzo identifikuju i odgovore na potencijalne pretnje. Stoga, interfejs mora podržavati bilo koju vrstu pretraživanja, sortiranja i filtriranja na svakom polju unutar IDMEF sadržaja. Ova funkcionalnost omogućava personalu da efektivno upravlja upozorenjima, prilagođavajući prikaz podataka svojim potrebama, i time značajno ubrzava proces odlučivanja. Uključivanjem ovih specifikacija, platforma za rano prepoznavanje IT incidenata postaje moćan alat koji ne samo da povećava sigurnost informacionog sistema, ali takođe značajno doprinosi optimalnom raspredelom resursa, jer omogućava IT stručnjacima da se fokusiraju na najkritičnije upozorenja i incidente, time povećavajući ukupnu efikasnost upravljanja informacionim sistemima. • Anonimizacija svih logova u skladu sa GDPR Kreiranje, uspostavljanje i održavanje jedinstvenog registra informacionih logova na ključnim elementima informacionog sistema, u okviru kojeg je neophodno pseudonimizirati i/ili anonimizirati sve prikupljene podatke u realnom vremenu, kao jednoj od ključne mere zaštite podataka o Anonimizacija podataka u realnom vremenu, čime se onemogućava bilo koji vid pretrage i skladištenja privatnih podataka korisnika sistema o Mogućnost otkrivanja anonimiziranih podataka, a na osnovu dodatnih informacija poznatih samo korisniku, na specifične ili zahteve u skladu sa zakonom. • Korelacija: o korelacija u realnom vremenu u cilju prepoznavanja poznatih vektora napada, a takođe i prepoznavanja anomalija u ponašanju na osnovu statističkih modela; o mogućnost „obogaćivanja" originalnih podataka na osnovu korelacije; o kreiranje „Skupovnih" događaja koji uključuju sve varijacije međusobno korealisanih događaja u događaju, isključujući potrebu za čuvanjem svih relevatnih događaja; o mogućnost adekvatne reakcije u cilju prevencije ili minimizacija posledica. o mogućnost implementairanja bilo koje poslovne logike u korelacionim pravilima; o Predefinisana baza korelacionih pravila , kao i mogućnost povezevanja na centralnu bazu korelacionih pravila proizvođača rešenja/platforme o istorijska korelacija za otkrivanje sporih, niskoprofilnih napada, kao i retroaktivne korelacije novootkrivenih vektora napada nad starim podacima; o integracija sa bazom VirusTotal(Virustotal) u cilju višestruke detekcije malicioznih/inficiranih procesa, a takođe i radi retroaktivne analize svih ikada startovanih procesa; o integracija sa javnim i komercijalnim threat intelligence sistemima u cilju korelacije sa lokalnim podacima i detekcije APT napada. • Vizuelna rekonstrukcija aktivnosti sistema/procesa/zaposlenih i mogućnost praćenja aktivnosti kroz vreme, a u cilju praćenja kompleksnih lanaca događaja radi lakše detekcije i forenzike napada. • Mogućnost vizuelnog praćenja aktivnosti administratora u realnom vremenu (praćenje pristupa sistemima, startovanih procesa, pristupa fajlovima i druge aktivnosti) i prikaz kroz interaktivne grafove. Raspoređivanje i praćenje sajber zamki Raspoređivanje i praćenje cyber zamki je potrebno u cilju proaktivne detekcije aktivnosti uljeza kod Naručioca. Zamke moraju biti podržane za svaku fazu napada, uključujući zamke na nivou operativnih sistema, mreža, lažnih servisa, memorije sistema, markiranih dokumenata. Raspoređivanje i praćenje cyber zamki podrazumeva sledeće: • Mogućnost postavljanja zamki koje simuliraju regularne sisteme a u cilju navođenja napadača na pogrešne korake, u cilju detekcije u realnom vremenu, svakog pokušaja i to vezano za lokaciju napadača (njegov IP i geolokaciju), način napada (vektor napada koji ukazuje na način na koji je izvršen napad (npr SQL injection string, vrsta logona...), kao i konkretne alatke koje napadač pokušava da uploaduje (malware, C&C programme, exploite..). • Zamke se postavljaju eksterno (na javnim IP adresama) ili interno (unutar korisničke LAN mreže). • Sledeće vrste zamki moraju da budu zadovoljene: o standardni servisi (zamke koje pružaju standardne servise kao što su samba, ftp, telnet, ssh, http i drugi), o digitalni klonovi: kloniranje specifičnog servisa u cilju otkrivanja njegovih ranjivosti i ranog otkrivanja napadača (npr kloniranje web kamera, web servisa, IoT uređaja...) o ubacivanje zamki u memoriju računara u cilju pogrešne detekcije postojećih servisa i korisničkih lozinki, o ubacivanje zamki u dokumente (doc, pdf) u cilju detekcije pokušaja otvaranje

dokumenta. • Sistem za praćenje aktivnosti na svim zamkama u realnom vremenu, sa geo mapom i identifikacijom geo lokacije odakle napad dolazi kao i praćenje statistike napada za svaku od zamki. • Centralna registracija svake zamke pre integracije u sistem, u cilju sprečavanja slanja lažnih informacija. • Mogućnost rada zamki na virtualnim mašinama kao i rada na eksternim uređajima. • Mogućnost pravljenja zamki po narudžbini, po specifičnim zahtevima. • Integracija zamki sa centralnim sistemom za praćenje, u cilju integracije podataka, korelacije sa drugim događajima u sistemu, vizuelne rekonstrukcije, kao i automatske remedijacije • Arhitektura: o mogućnost distribuiranog procesiranja: mogućnost horizontalne skalabilnosti Sistema tako da se određene faze procesiranje mogu izvršavati paralelno na različitim sistemima; o dinamičko rutiranje događaja: mogućnost rutiranja događaja na različite putanje procesiranja u zavisnosti od sadržaja samog događaja; o kompletan sistem mora podražavati izvršavanje na virtuelnim mašinama. * Broj radnih stanica je 100, sa mogućim proširenjem do 200.

CIJENA I USLOVI PLAĆANJA

Član 2

Ukupna vrijednost robe, prema prihvaćenoj ponudi br : 111634od 19.09.2024.g.g

- Ukupno bez PDV-a: 24900€
- PDV: 5229€

Ukupan iznos **sa PDV-om: 30 129,00€**
Slovima : tridesethiljadastodvadesetdeveteura i 00/100

Član 3

Mjesto realizacije ugovora, fco narucilac.Mesto isporuke, ugradnje i instalacije (hardverske platforme): objekat Naručioca u Herceg Novom

U cijenu su uključeni svi troškovi koji prate predmetnu javnu nabavku fco Naručilac.

Član 4

Ugovorne strane su saglasne da će NARUČILAC izvršiti plaćanje po sukcesivnom izvršenju predmeta javne nabavke u roku od 15 dana od dana prijema facture, nakon Zapisnika o primopredaji posla i obuke dva radnika Naručioca, prema ponudi. Isplata se vrši sa računa naručioca.

Sve uplate se vrše u korist žiro računa izvrsioca usluga:

RS35265100000024719822 ADVANCED CYBER SECURITY

ROK ISPORUKE

Član 5

IZVRŠILAC USLUGA se obavezuje da ugovorenu komplet uslugu izvrši u roku od 30 dana od dana potpisivanja ugovora .

Datum realizacije ugovora sa izvršenim uslugama je datum potpisivanja zapisnika o kvantitativnom i kvalitetivnom prijemuusluge, nakon provjere kompletnosti i funkcionalnosti koju treba da izvrši NARUČIOC , na lokaciji NARUČIOCA, uz prisustvo ovlašćenih predstavnika IZVRŠIOCA USLUGA. Po završetku kvalitativno-kvantitativne primopredaje Komisija je obavezna da sačini zapisnik.koji potpisuju i ovjeravaju predstavnici ugovornih strana.

Način komunikacije za predmetnu javnu nabavku je e-mail naručioca i ponuđača, koji se mora obezbjediti , da bude neometan.

Ponuđač predajom ponude i izvrsenim poslom usluga, garantuje da će predmet nabavke biti u skladu sa ponudom , ugovorom, propisima , normativima,standardima za ovu vrstu robe i posla, pravilima struke i potrebama Naručioca

(vrsta ,količina) i da neće imati mana koje onemogućavaju ili umanjuju njihovu vrednost ili njihovu podobnost za redovnu upotrebu, odnosno upotrebu određenu predmetnim ugovorom,

RASKID UGOVORA

Član 6

Ugovorne strane su saglasne da do raskida ovog Ugovora može doći ako IZVRŠILAC USLUGA ne bude izvršavao svoje obaveze u rokovima i na način predvidjen Ugovorom:

- U slučaju kada NARUČILAC ustanovi da kvalitet robe koja je predmet ovog ugovora ili način na koje se isporučuje, odstupa od traženog, odnosno ponudjenog kvaliteta iz ponude IZVRŠIOCA USLUGA,
- U slučaju da se IZVRŠILAC USLUGA ne pridržava svojih obaveza i u drugim slučajevima nesavjesnog obavljanja posla. Isto pravo NARUČILAC ima u slučaju raskida ugovora, do izbora novog IZVRŠIOCA USLUGA .
- Naručilac je obavezan da u slučaju uočavanja propusta u obavljanju posla pisanim putem pozove DOBAVLJAČA i da putem Zapisnika zajednički konstatuju uzrok i obim uočenih propusta.

Član 7

Za sve što nije definisano ovim ugovorom primjenjivaće se odredbe Zakona o obligacionim odnosima.

UGOVORNA KAZNA

Član 8

IZVRŠILAC USLUGA se obavezuje da plati ugovornu kaznu u visini 2‰ za svaki dan kašnjenja u isporuci opreme, a najviše 5% od ukupne vrijednosti ugovorenog posla.

GARANCIJA

Član 9

IZVRŠILAC USLUGA garantuje da predmetne usluge neće imati nedostataka.

IZVRŠILAC USLUGA garantuje kvalitet iizvrsene usluge i obavezuje se da bez odlaganja, o svom trošku, otkloni svaki kvar ili problem koji nije posledica nepravilnog rada NARUČIOCA.

NARUČILAC je u obavezi da svaki problem u radu ili kvar pisano prijavi IZVRŠIOCU USLUGA(putem fax sistema , putem e-mail –a, odmah po njenom nastanku.

Usluge prevencije sajber napada se odnosi na korišćenje centra za rano prepoznavanja IT incidenata, što treba da doprinese sveukupnom povećanju bezbednosti postojećih IT sistema Od ponuđača se očekuje uspostavljanje sistema koji u realnom vremenu prikuplja podatke sa svih kritičnih sistema, prepoznaje incidente i na adekvatan način o njima obaveštava Naručioca.

Izvrsilac usluga mora da: • čuva kao poverljive sve informacije vezane za bezbednosnu infrastrukturu Naručioca, kao i sve druge informacije sa kojima dođe u kontakt tokom perioda pružanja usluge, u skladu sa Zakonima koji pokrivaju predmetnu oblast • Garantuje mogućnost izmene koda u smislu promene ili dodavanja novih funkcionalnosti na zahtev Naručioca. • Obezbedi tehničku podršku i održavanje platforme za rano prepoznavanje IT incidenata

Tehnička podrška ponuđača putem e-pošte i telefona 24h7 (24 (dvadeset četiri) sati dnevno, sedam dana u nedelji) koja podrazumeva dobijanje odgovora na sva pitanja vezana za optimalno funkcionisanje i administraciju platforme za rano prepoznavanje IT incidenata, na period od 12 (dvanaest) meseci.

Korektivno održavanje Pod korektivnim održavanjem podrazumeva se otklanjanje nefunkcionalnosti u radu platforme za rano prepoznavanje IT incidenata. Korektivno održavanje podrazumeva udaljenu (remote) i podršku na lokaciji Naručioca (onsite) u slučaju neispravnosti, nefunkcionisanja i kvarova implementiranog softvera za monitoring, zaštitu i prikupljanje podataka. Ponuđač je dužan da prati rad sistema i da izvršava sve potrebne aktivnosti na otklanjanju neispravnosti, nefunkcionisanja i kvarova implementiranog softvera za monitoring, zaštitu i prikupljanje podataka, odnosno da vrši sve potrebne aktivnosti u svrhu obezbedivanja pune funkcionalnosti, u periodu od 12 (dvanaest) meseci.

Izvrsilac usluga organizuje i izvrši obuku za rad u centru za rano prepoznavanja IT incidenata za 2 zaposlena lica Naručioca.

Izvršilac usluga će omogućiti izmene koda u smislu promene ili dodavanja novih funkcionalnosti na zahtev Naručioca; - na period od 12 (dvanaest) meseci ce obezbediti tehničku podršku putem e-pošte i telefona, korektivno održavanje i redundatni Centar za rano prepoznavanje IT incidenata.

Član 10

Rok odziva po prijavi tehničkog problema: maksimalno 1 sat od prijave istog putem maila u garantnom periodu. Ponuđač mora obezbjediti neometani prijem maila.

Rok za otklanjanje kvara/nedostatka na opremi u garantnom roku: 24 sata od sata od sata odziva po prijavi kvara.

Garantni rok za pruženu uslugu: 12 (dvanaest) meseci i važi od dana potpisivanja Zapisnika o pruženoj usluzi.

Broj radnih stanica koje naručilac sada ima je 100, sa mogućim proširenjem do 200.

OBAVEZE NARUČIOCA

Član 11

NARUČILAC se obavezuje da obezbjedi prostor i uslove za isporuku ugovorene robe.

PREUZIMANJE PRAVA I OBAVEZA

Član 12

Ukoliko u toku važnosti ovog ugovora dođe do bilo kakvih promjena u nazivu ili drugim statusnim promjenama ugovornih strana, tada će sva prava i obaveze ugovorne strane kod koje dođe do takve promjene, preći na njenog pravnog sljedbenika.

PRIMJENA PROPISA

Član 13

Za sve što ne predvidjeno ovim ugovorom primjenjuju se odredbe Zakona o obligacionim odnosima i drugih pozitivnih propisa.

SUDSKA NADLEŽNOST

Član 14

Ugovorne strane su saglasne da eventualne sporove povodom ovog ugovora rješavaju sporazumom. U protivnom, ugovara se nadležnost suda u Podgorici

PRIMJERCI UGOVORA

Član 15

Ovaj ugovor je pravno valjano zaključen i potpisan od dolje navedenih ovlašćenih zakonskih zastupnika strana ugovora i sačinjen je u 6 (šest) istovjetnih primjeraka, od kojih po 3 (tri) primjerka za NARUČIOCA i IZVRŠIOCA USLUGA.

Član 16

Ugovor o javnoj nabavci koji je zaključen uz kršenje **antikorupcijskog pravila ništav** je, u smislu člana 38,stav 3 , Zakona o javnim nabavkama („Službeni list CG", br. 074/19,3/23 , 49/23) .

NARUČILAC

Doo" Vodovod i kanalizacija"

Herceg Novi

Izvršni direktor

Boro Lučić

IZVRŠILAC USLUGA

ADVANCED CYBER SECURITY doo

Beograd, RSrbija

Herceg Novi

Izvršni direktor

Aleksandar Kotevski